

UNITED STATES DISTRICT COURT
for the
Southern District of New York

In the Matter of the Search of)
 (Briefly describe the property to be searched)
 or identify the person by name and address)
 the Contents of an iCloud Account)
 Currently Located on a Hard Drive Partition)
 Containing the Results of a Prior Search Warrant)
) Case No.

20 MAG 3074

WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search and seizure of the following person or property located in the Southern District of New York (identify the person or describe the property to be searched and give its location):

See Attachment A

The search and seizure are related to violation(s) of (insert statutory citations):

52 U.S.C. § 30122, 52 U.S.C. § 30121, 18 U.S.C. § 371, 18 U.S.C. § 2, 18 U.S.C. § 1001, 18 U.S.C. § 1001 and 2, 18 U.S.C. § 1519, 22 U.S.C. §§ 612 and 618, 18 U.S.C. § 951, 18 U.S.C. § 1956 and 18 U.S.C. § 1343

I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or property described above, and that such search will reveal (identify the person or describe the property to be seized):

See Attachment A

YOU ARE COMMANDED to execute this warrant on or before April 3, 2020 (not to exceed 14 days)
 in the daytime 6:00 a.m. to 10:00 p.m. at any time in the day or night because good cause has been established.

Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property taken to the person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the property was taken.

The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory as required by law and promptly return this warrant and inventory to the Clerk of the Court

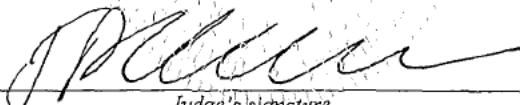
(United States Magistrate Judge)

Pursuant to 18 U.S.C. § 3103a(b), I find that immediate notification may have an adverse result listed in 18 U.S.C. § 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose property, will be searched or seized (check the appropriate box)

for days (not to exceed 30) until, the facts justifying, the later specific date of

Date and time issued:

March 20, 2020
12:05 PM


Judge's signature

City and state: New York, NY

Hon. J. Paul Oetken
Printed name and title

AO 93C (08/18) Warrant by Telephone or Other Reliable Electronic Means (Page 2)

Return

| | | |
|-----------|---------------------------------|--|
| Case No.: | Date and time warrant executed: | Copy of warrant and inventory left with: |
|-----------|---------------------------------|--|

Inventory made in the presence of :

Inventory of the property taken and name(s) of any person(s) seized:

Certification

I declare under penalty of perjury that this inventory is correct and was returned along with the original warrant to the designated judge.

Date: _____

*Executing officer's signature**Printed name and title*

Attachment A

I. Device Subject to Search and Seizure

The device that is the subject of this search and seizure warrant (the "Subject Device") is described as follows:

a hard drive partition in the possession of the FBI which contains the results of an October 21, 2019 search warrant for the Apple iCloud account assigned identification number [REDACTED].

II. Review of ESI on the Subject Device

Law enforcement personnel (who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, agency personnel assisting the government in this investigation, and outside technical experts under government control) are authorized to review the ESI contained on the Subject Device for evidence, fruits, and instrumentalities of violations of 52 U.S.C. § 30122 (unlawful straw donations), 52 U.S.C. § 30121 (unlawful contribution by a foreign national), 18 U.S.C. § 371 (conspiracy to commit the same), 18 U.S.C. § 2 (aiding and abetting the same), 18 U.S.C. § 1001 (false statement to the Federal Election Commission ("FEC")), and 18 U.S.C. § 1001 and 2 (willfully causing a false statement to be made to the FEC), 18 U.S.C. § 1519 (fabrication of documents); 22 U.S.C. §§ 612 and 618 (failure to register as a foreign agent); 18 U.S.C. § 951 (acting as an agent of a foreign government); 18 U.S.C. § 1956 (international promotional money laundering); and 18 U.S.C. § 1343 (wire fraud) (the "Subject Offenses"), limited to content created, sent, or received between September 1, 2016 and October 21, 2019, as listed below:

- a. Evidence relating to the creation, incorporation, or operation of Global Energy Producers ("GEP"), or other shell corporations used to make political contributions.
- b. Evidence relating to the ownership of GEP, including any evidence relating to attempts to conceal the ownership of GEP.
- c. Evidence necessary to establish the extent to which GEP is operating as an actual business, including as an oil, gas, or energy business.
- d. Evidence relating to the funding of bank accounts held in the name of GEP.
- e. Evidence relating to political contributions made by Fruman, Parnas, their family members, GEP, and its affiliates, employees, or representatives, or other entities controlled by Fruman and Parnas.
- f. Evidence relating to the source of the funds used to make any political contributions by Fruman, Parnas, their family members, GEP, and its affiliates, employees, or representatives, or other entities controlled by Fruman and Parnas.

g. Evidence relating to the sources of the funds deposited into bank accounts held by Fruman, Igor Fruman's brother (██████████ Correia, or Parnas, or on which those individuals are listed as a signatory.

h. Evidence of other bank accounts or entities related to GEP, Parnas, Igor Fruman, ██████████ and ██████████ including emails reflecting registration of other accounts potentially containing relevant evidence.

i. Evidence relating to communications with or regarding political candidates, campaigns, political action committees, political consultants, or political contributions.

j. Evidence relating to communications with ██████████ (██████████ or Andrey Muraviev.

k. Evidence relating to contributions made in the name “██████████”

l. Evidence relating to contributions to any federal, state, or local candidate, or any political action committee, including but not limited to ██████████ PAC, ██████████ PAC, ██████████ PAC, the ██████████ Fund, ██████████ Fund, or ██████████ for Congress, ██████████ for Congress, the ██████████ Fund, or ██████████

m. Evidence of intent to make unlawful political contributions or violate the campaign finance laws.

n. Evidence related to any false statements made or caused to be made to the Federal Election Commission.

o. Evidence of knowledge of the campaign finance laws, including but not limited to knowledge of the prohibition of making contributions in the name of another person, and knowledge of the prohibition on contributions by foreign nationals.

p. Evidence relating to the May 9, 2018 letter from Congressman ██████████ to Secretary of State ██████████ regarding U.S. Ambassador ██████████ including correspondence attaching or concerning the letter.

q. Communications with individuals associated with the government or a political party in the Ukraine, including ██████████, ██████████, or ██████████.

r. Communications regarding ██████████ specifically or the position of U.S. Ambassador to Ukraine generally.

s. Evidence, including travel records, related to meetings with Ukrainian government officials involving Rudolph Giuliani, ██████████ Parnas, or Fruman.

t. Evidence of knowledge of the foreign agent registration laws and requirements, or lobbying laws, including but not limited to knowledge of the requirement to register as an agent

of a foreign principal, or of the prohibition of acting on behalf of, lobbying for, or making contributions on behalf of a foreign principal.

u. Passwords or other information needed to access user's online accounts.

v. Evidence of the intent of Parnas, Igor Fruman, [REDACTED], David Correia, Andrey Kukushkin, Andrey Muraviev, Giuliani, [REDACTED] [REDACTED] and [REDACTED] [REDACTED] as it relates to the Subject Offenses under investigation.

UNITED STATES DISTRICT COURT
 for the
 Southern District of New York

In the Matter of the Search of
 (Briefly describe the property to be searched
 or identify the person by name and address))
 the Contents of an iCloud Account)
 Currently Located on a Hard Drive Partition)
 Containing the Results of a Prior Search Warrant)
)
)
 Case No.

APPLICATION FOR A WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):

See Attachment A

located in the Southern District of New York, there is now concealed (identify the person or describe the property to be seized):

See Attachment A

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

evidence of a crime;
 contraband, fruits of crime, or other items illegally possessed;
 property designed for use, intended for use, or used in committing a crime;
 a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section

Offense Description

52 U.S.C. § 30122, 52 U.S.C. § 30121, 18 U.S.C. § 371, 18 U.S.C. § 2, 18 U.S.C. § 1001, 18 U.S.C. § 1001 and 2, 18 U.S.C. § 1519, 22 U.S.C. §§ 612 and 618, 18 U.S.C. § 951, 18 U.S.C. § 1956 and 18 U.S.C. § 1343

The application is based on these facts:

See attached affidavit.

Continued on the attached sheet.
 Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by
 telephone _____ (specify reliable electronic means).

Date: 03/20/2020


 Judge's signature

City and state: New York, NY

Hon. J. Paul Oetken

Printed name and title

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

In the Matter of the Application of the United States of America for a Search and Seizure Warrant for the Contents of an iCloud Account Currently Located on a Hard Drive Partition Containing the Results of a Prior Search Warrant; USAO Reference No. [REDACTED]

TO BE FILED UNDER SEAL

**Agent Affidavit in Support of
Application for Search and Seizure
Warrant**

SOUTHERN DISTRICT OF NEW YORK) ss.:

[REDACTED], being duly sworn, deposes and says:

I. Introduction

A. Affiant

1. I am a Special Agent with the Federal Bureau of Investigation (“FBI”). In the course of my experience and training in this position, I have participated in criminal investigations into federal offenses involving public corruption and violations of the federal campaign finance laws. I also have training and experience executing search warrants, including those involving electronic evidence, including emails.

2. I make this Affidavit in support of an application pursuant to Rule 41 of the Federal Rules of Criminal Procedure for a warrant to search the electronic device specified below (the “Subject Device”) for the items and information described in Attachment A. This affidavit is based upon my personal knowledge; my review of documents and other evidence; my conversations with other law enforcement personnel; and my training, experience and advice received concerning the use of computers in criminal activity and the forensic analysis of electronically stored information (“ESI”). Because this affidavit is being submitted for the limited purpose of establishing probable cause, it does not include all the facts that I have learned during the course of my investigation.

Where the contents of documents and the actions, statements, and conversations of others are reported herein, they are reported in substance and in part, except where otherwise indicated.

B. The Subject Device and its Contents

3. The Subject Device is particularly described as a hard drive partition in the possession of the FBI which contains the results of a search warrant for the Apple iCloud account assigned identification number [REDACTED], which is registered to Igor Fruman (the “Fruman iCloud Account”). The data on the Subject Device was obtained from Apple, Inc. pursuant to an October 21, 2019, search warrant (the “October 21 Warrant,” as described further below).

4. The Subject Device is presently located in the Southern District of New York.

C. The Subject Offenses

5. As detailed below, there is probable cause to believe that the Subject Device contains evidence, fruits, and instrumentalities of violations of 52 U.S.C. § 30122 (unlawful straw donations), 52 U.S.C. § 30121 (unlawful contribution by a foreign national), 18 U.S.C. § 371 (conspiracy to commit the same), 18 U.S.C. § 2 (aiding and abetting the same), 18 U.S.C. § 1001 (false statement to the Federal Election Commission (“FEC”)), and 18 U.S.C. § 1001 and 2 (willfully causing a false statement to be made to the FEC), 18 U.S.C. § 1519 (fabrication of documents); 18 U.S.C. § 1956 (international promotional money laundering); and 18 U.S.C. § 1343 (wire fraud) (collectively, the “Campaign Finance Offenses”), as well as 22 U.S.C. §§ 612 and 618 (failure to register as a foreign agent); and 18 U.S.C. § 951 (acting as an agent of a foreign government) (collectively, the “FARA Offenses,” and together with the Campaign Finance Offenses, the “Subject Offenses”).

II. Probable Cause

A. Probable Cause Justifying Search of the Subject Device

6. On or about May 16, 2019, the United States Attorney's Office and FBI sought and obtained from the Honorable Stewart Aaron, Magistrate Judge for the Southern District of New York, a search warrant (the "May 16 Warrant") for the Fruman iCloud Account. The May 16 Warrant authorized law enforcement personnel to search the Fruman iCloud Account for evidence of the Campaign Finance Offenses and specified that law enforcement personnel were authorized to seize evidence created or modified between September 1, 2016 and the date of the warrant. A copy of the warrant and affidavit are attached hereto as Exhibit 1.

7. In response to the May 16 Warrant, Apple provided data to the FBI. While the data included multimedia and non-content information, it lacked records of communications, such as iMessages or WhatsApp messages.

8. On or about October 17, 2019, the Honorable J. Paul Oetken, District Judge of the Southern District of New York, signed a warrant authorizing the search of the data previously obtained for the Fruman iCloud Account for evidence of the FARA Offenses (the "October 17 Warrant"). A copy of that warrant and affidavit are attached hereto as Exhibit 2.

9. On or about October 21, 2019, the USAO and FBI sought and obtained from Judge Oetken a search warrant (the "October 21 Warrant") for the Fruman iCloud Account. The October 21 Warrant authorized law enforcement personnel to search the Fruman iCloud Account for evidence of the Subject Offenses and specified that law enforcement personnel were authorized to seize evidence created or modified between May 1, 2019 and the date of the warrant. A copy of that warrant and affidavit are attached hereto as Exhibit 3.

10. In response to the October 21 Warrant, Apple provided data to the FBI. Unlike its prior production, Apple's production did include communications, including iMessages and

WhatsApp messages. Because it is Apple's practice to produce all records associated with an account, it appears that the returns include communications since at least October 2016 and extending to the date of the warrant.

11. For the reasons set forth in the affidavits to the May 21 Warrant, the October 17 Warrant, and the October 21 Warrant, there is probable cause to believe that the Fruman iCloud Account—and therefore the data from that account on the Subject Device—will contain evidence of the Subject Offenses for the period September 1, 2016 to October 21, 2019.

B. Evidence, Fruits and Instrumentalities

12. Based upon the foregoing, including the information set forth in the May 21 Warrant, the October 17 Warrant, and the October 21 Warrant, I respectfully submit there is probable cause to believe that the Subject Device will contain evidence, fruits, and instrumentalities of the Subject Offenses, as more fully described in Section II of Attachment A to the proposed warrant. In particular, I believe the Subject Device is likely to contain the following information:¹

- a. Evidence relating to the creation, incorporation, or operation of Global Energy Producers (“GEP”), or other shell corporations used to make political contributions.
- b. Evidence relating to the ownership of GEP, including any evidence relating to attempts to conceal the ownership of GEP.
- c. Evidence necessary to establish the extent to which GEP is operating as an actual business, including as an oil, gas, or energy business.
- d. Evidence relating to the funding of bank accounts held in the name of GEP.

¹ This is the same information that was sought by the October 21 Warrant.

e. Evidence relating to political contributions made by Fruman, Parnas, their family members, GEP, and its affiliates, employees, or representatives, or other entities controlled by Fruman and Parnas.

f. Evidence relating to the source of the funds used to make any political contributions by Fruman, Parnas, their family members, GEP, and its affiliates, employees, or representatives, or other entities controlled by Fruman and Parnas.

g. Evidence relating to the sources of the funds deposited into bank accounts held by Fruman, Igor Fruman's brother (██████████ Correia, or Parnas, or on which those individuals are listed as a signatory.

h. Evidence of other bank accounts or entities related to GEP, Parnas, Igor Fruman, ██████████ and ██████████ including emails reflecting registration of other accounts potentially containing relevant evidence.

i. Evidence relating to communications with or regarding political candidates, campaigns, political action committees, political consultants, or political contributions.

j. Evidence relating to communications with ██████████ or Andrey Muraviev.

k. Evidence relating to contributions made in the name “██████████”

l. Evidence relating to contributions to any federal, state, or local candidate, or any political action committee, including but not limited to ██████████ PAC, ██████████

██████████ PAC, ██████████ PAC, the ██████████ Fund, ██████████ for Congress, ██████████ for Congress, the ██████████ Fund, ██████████ or ██████████

m. Evidence of intent to make unlawful political contributions or violate the campaign finance laws.

n. Evidence related to any false statements made or caused to be made to the Federal Election Commission.

o. Evidence of knowledge of the campaign finance laws, including but not limited to knowledge of the prohibition of making contributions in the name of another person, and knowledge of the prohibition on contributions by foreign nationals.

p. Evidence relating to the May 9, 2018 letter from Congressman [REDACTED] to Secretary of State [REDACTED] regarding U.S. Ambassador [REDACTED], including correspondence attaching or concerning the letter.

q. Communications with individuals associated with the government or a political party in the Ukraine, including [REDACTED], [REDACTED], or [REDACTED].

r. Communications regarding [REDACTED] specifically or the position of U.S. Ambassador to Ukraine generally.

s. Evidence, including travel records, related to meetings with Ukrainian government officials involving Rudolph Giuliani, [REDACTED] Parnas, or Fruman.

t. Evidence of knowledge of the foreign agent registration laws and requirements, or lobbying laws, including but not limited to knowledge of the requirement to register as an agent of a foreign principal, or of the prohibition of acting on behalf of, lobbying for, or making contributions on behalf of a foreign principal.

u. Passwords or other information needed to access user's online accounts.

Evidence of the intent of Parnas, Igor Fruman, [REDACTED], David Correia, Andrey Kukushkin, Andrey Muraviev, Giuliani, [REDACTED], as it relates to the Subject Offenses under investigation.

III. Procedures for Searching ESI

A. Review of ESI

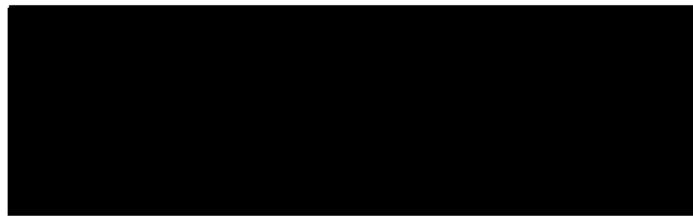
13. Law enforcement personnel (who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, agency personnel assisting the government in this investigation, and outside technical experts under government control) will review the ESI contained on the Subject Device for information responsive to the warrant.

14. In conducting this review, law enforcement personnel may use various methods to locate evidence, fruits, and instrumentalities of the Subject Offenses, including but not limited to undertaking a cursory inspection of all records within the Subject Device. This method is analogous to cursorily inspecting all the files in a file cabinet in an office to determine which paper evidence is subject to seizure. Although law enforcement personnel may use other methods as well, particularly including keyword searches, I know that keyword searches and similar methods are typically inadequate to detect all information subject to seizure. As an initial matter, keyword searches work only for text data, yet many types of files commonly associated with emails, including attachments such as scanned documents, pictures, and videos, do not store data as searchable text. Moreover, even as to text data, keyword searches cannot be relied upon to capture all relevant communications in an account, as it is impossible to know in advance all of the unique words or phrases that investigative subjects will use in their communications, and consequently there are often many communications in an account that are relevant to an investigation but that do not contain any keywords that an agent is likely to search for.

IV. Conclusion and Ancillary Provisions

15. Based on the foregoing, I respectfully request the court to issue a warrant to seize the items and information specified in Attachment A to this affidavit and to the Search and Seizure Warrant.

16. In light of the confidential nature of the continuing investigation, I respectfully request that this affidavit and all papers submitted herewith be maintained under seal until the Court orders otherwise.



Sworn to before me on
20 day of March, 2020


HON. J. PAUL OETKEN
UNITED STATES DISTRICT JUDGE

Attachment A

I. Device Subject to Search and Seizure

The device that is the subject of this search and seizure warrant (the “Subject Device”) is described as follows:

a hard drive partition in the possession of the FBI which contains the results of an October 21, 2019 search warrant for the Apple iCloud account assigned identification number [REDACTED].

II. Review of ESI on the Subject Device

Law enforcement personnel (who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, agency personnel assisting the government in this investigation, and outside technical experts under government control) are authorized to review the ESI contained on the Subject Device for evidence, fruits, and instrumentalities of violations of 52 U.S.C. § 30122 (unlawful straw donations), 52 U.S.C. § 30121 (unlawful contribution by a foreign national), 18 U.S.C. § 371 (conspiracy to commit the same), 18 U.S.C. § 2 (aiding and abetting the same), 18 U.S.C. § 1001 (false statement to the Federal Election Commission (“FEC”)), and 18 U.S.C. § 1001 and 2 (willfully causing a false statement to be made to the FEC), 18 U.S.C. § 1519 (fabrication of documents); 22 U.S.C. §§ 612 and 618 (failure to register as a foreign agent); 18 U.S.C. § 951 (acting as an agent of a foreign government); 18 U.S.C. § 1956 (international promotional money laundering); and 18 U.S.C. § 1343 (wire fraud) (the “Subject Offenses”), limited to content created, sent, or received between September 1, 2016 and October 21, 2019, as listed below:

- a. Evidence relating to the creation, incorporation, or operation of Global Energy Producers (“GEP”), or other shell corporations used to make political contributions.
- b. Evidence relating to the ownership of GEP, including any evidence relating to attempts to conceal the ownership of GEP.
- c. Evidence necessary to establish the extent to which GEP is operating as an actual business, including as an oil, gas, or energy business.
- d. Evidence relating to the funding of bank accounts held in the name of GEP.
- e. Evidence relating to political contributions made by Fruman, Parnas, their family members, GEP, and its affiliates, employees, or representatives, or other entities controlled by Fruman and Parnas.
- f. Evidence relating to the source of the funds used to make any political contributions by Fruman, Parnas, their family members, GEP, and its affiliates, employees, or representatives, or other entities controlled by Fruman and Parnas.

g. Evidence relating to the sources of the funds deposited into bank accounts held by Fruman, Igor Fruman's brother (██████████ Correia, or Parnas, or on which those individuals are listed as a signatory.

h. Evidence of other bank accounts or entities related to GEP, Parnas, Igor Fruman, ██████████ and ██████████, including emails reflecting registration of other accounts potentially containing relevant evidence.

i. Evidence relating to communications with or regarding political candidates, campaigns, political action committees, political consultants, or political contributions.

j. Evidence relating to communications with ██████████ or Andrey Muraviev.

k. Evidence relating to contributions made in the name of ██████████

l. Evidence relating to contributions to any federal, state, or local candidate, or any political action committee, including but not limited to ██████████ PAC, ██████████ ██████████ PAC, ██████████ PAC, the ██████████ Fund, ██████████ Fund, ██████████ for Congress, ██████████ for Congress, the ██████████ Fund, ██████████ or ██████████

m. Evidence of intent to make unlawful political contributions or violate the campaign finance laws.

n. Evidence related to any false statements made or caused to be made to the Federal Election Commission.

o. Evidence of knowledge of the campaign finance laws, including but not limited to knowledge of the prohibition of making contributions in the name of another person, and knowledge of the prohibition on contributions by foreign nationals.

p. Evidence relating to the May 9, 2018 letter from Congressman ██████████ to Secretary of State ██████████ regarding U.S. Ambassador ██████████, including correspondence attaching or concerning the letter.

q. Communications with individuals associated with the government or a political party in the Ukraine, including ██████████

r. Communications regarding ██████████ specifically or the position of U.S. Ambassador to Ukraine generally.

s. Evidence, including travel records, related to meetings with Ukrainian government officials involving Rudolph Giuliani, ██████████ Parnas, or Fruman.

t. Evidence of knowledge of the foreign agent registration laws and requirements, or lobbying laws, including but not limited to knowledge of the requirement to register as an agent

of a foreign principal, or of the prohibition of acting on behalf of, lobbying for, or making contributions on behalf of a foreign principal.

u. Passwords or other information needed to access user's online accounts.

v. Evidence of the intent of Parnas, Igor Fruman, [REDACTED], David Correia, Andrey Kukushkin, Andrey Muraviev, Giuliani, [REDACTED] and [REDACTED] as it relates to the Subject Offenses under investigation.

Exhibit 1

(May 16, 2019 Warrant and Application)

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

19MAG4784

In the Matter of a Warrant for All Content and
Other Information Associated with the iCloud
Accounts with Apple IDs [REDACTED]
[REDACTED] and [REDACTED]
Maintained at Premises Controlled by Apple,
Inc., USAO Reference No. [REDACTED]

SEARCH WARRANT AND NON-DISCLOSURE ORDER

TO: Apple Inc. ("Provider")

United States Attorney's Office for the Southern District of New York and the Federal Bureau of Investigation (collectively, the "Investigative Agencies")

1. Warrant. Upon an affidavit of Special Agent [REDACTED] of the Federal Bureau of Investigation, and pursuant to the provisions of the Stored Communications Act, 18 U.S.C. § 2703(b)(1)(A) and § 2703(c)(1)(A), and the relevant provisions of Federal Rule of Criminal Procedure 41, the Court hereby finds there is probable cause to believe the iCloud Accounts with Apple IDs [REDACTED] maintained at premises [REDACTED] controlled by Apple Inc., contain evidence, fruits, and instrumentalities of crime, all as specified in Attachment A hereto. Accordingly, the Provider is hereby directed to provide to the Investigative Agencies, within 10 days of the date of service of this Warrant and Order, the records specified in Section II of Attachment A hereto, for subsequent review by law enforcement personnel as authorized in Section III of Attachment A. The Government is required to serve a copy of this Warrant and Order on the Provider within 14 days of the date of issuance. The Warrant and Order may be served via electronic transmission or any other means through which the Provider is capable of accepting service.

2. Non-Disclosure Order. Pursuant to 18 U.S.C. § 2705(b), the Court finds that there is reason to believe that notification of the existence of this warrant will result in destruction of or tampering with evidence, and/or tamping with potential witnesses, or otherwise will seriously jeopardize an ongoing investigation. Accordingly, it is hereby ordered that the Provider shall not disclose the existence of this Warrant and Order to the listed subscriber or to any other person for a period of one year from the date of this Order, subject to extension upon application to the Court if necessary, except that Provider may disclose this Warrant and Order to an attorney for Provider for the purpose of receiving legal advice.

3. Sealing. It is further ordered that this Warrant and Order, and the Affidavit upon which it was issued, be filed under seal, except that the Government may without further order of this Court serve the Warrant and Order on the Provider; provide copies of the Affidavit or Warrant and Order as need be to personnel assisting the Government in the investigation and prosecution of this matter; and disclose these materials as necessary to comply with discovery and disclosure obligations in any prosecutions related to this matter.

Dated: New York, New York

5/16/2019
Date Issued

2:16pm
Time Issued


UNITED STATES MAGISTRATE JUDGE
Southern District of New York

iCloud Search Warrant Attachment A

I. Subject Account and Execution of Warrant

This warrant is directed to Apple Inc. (the “Provider”), headquartered at 1 Infinite Loop, Cupertino, California 95014, and applies to all content and other information within the Provider’s possession, custody, or control associated with the iCloud accounts with Apple IDs [REDACTED], [REDACTED] (the “Subject Accounts”). The Provider is directed to produce the information described below associated with the Subject Accounts for the period September 1, 2016 through the date of this warrant.

A law enforcement officer will serve this warrant by transmitting it via email or another appropriate manner to the Provider. The Provider is directed to produce to the law enforcement officer an electronic copy of the information specified in Section II below. Upon receipt of the production, law enforcement personnel will review the information for items falling within the categories specified in Section III below.

II. Information to be Produced by the Provider

To the extent within the Provider’s possession, custody, or control, the Provider is directed to produce the following information associated with the Subject Accounts:

- a. *Subscriber and payment information.* All subscriber and payment information regarding the Subject Accounts, including but not limited to name, username, address, telephone number, alternate email addresses, registration IP address, account creation date, account status, length of service, types of services utilized, means and source of payment, and payment history.
- b. *Device information and settings.* All information about the devices associated with the Subject Accounts, including but not limited to the Integrated Circuit Card ID (“ICCID”) number, the Media Access Control address (“MAC address”), the unique device identifier (“UDID”), the serial number, customer device settings, and repair history.

- c. *Transactional records.* All transactional records associated with the Subject Accounts, including any IP logs or other records of session times and durations.
- d. *Purchase records.* All purchase records associated with the Subject Accounts, including records reflecting app purchases from the App Store and/or iTunes Store.
- e. *Address book information.* All address book, contact list, or similar information associated with the Subject Accounts.
- f. *Call history and voicemails.* All call histories, logs for FaceTime calls, audio voicemails, and visual voicemails associated with the Subject Accounts.
- g. *Text message content.* All text messages (including iMessages, Short Message Service (“SMS”) messages, and Multimedia Messaging Service (“MMS”) messages) sent to or from, stored in draft form in, or otherwise associated with the Subject Accounts, including all message content, attachments, and header information (specifically including the source and destination addresses associated with each text message, and the date and time at which each text message was sent).
- h. *Email content.* All emails sent to or from, stored in draft form in, or otherwise associated with the Subject Accounts, including all message content, attachments, and header information (specifically including the source and destination addresses associated with each email, the date and time at which each email was sent, and the size and length of each email).
- i. *Photos and videos.* All photographs or videos associated with the Subject Accounts, including any photographs or videos found on any iCloud Photo Library, My Photo Stream, or iCloud Photo Sharing service linked to the Subject Accounts. All associated metadata with any photograph or video including the time and date of creation, the author or creator, the means of its creation, and the GPS location information for where a photo or video was taken.

j. *Documents.* All documents stored in or otherwise associated with the Subject Accounts, including all documents in iCloud Drive, and iWork Apps.

k. *Search and web histories.* All search history, web history, bookmarks, and iCloud Tabs.

l. *Third-party application data.* All records, messages, and data relating to third-party applications, including WhatsApp and other third-party messaging applications, stored in or otherwise associated with the Subject Accounts.

m. *Location data.* All location data associated with the Subject Accounts.

n. *Customer correspondence.* All correspondence with the subscriber or others associated with the Subject Accounts, including complaints, inquiries, or other contacts with support services and records of actions taken.

III. Review of Information by the Government

Law enforcement personnel (who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, agency personnel assisting the government in this investigation, and outside technical experts under government control) are authorized to review the records produced by the Provider in order to locate any evidence, fruits, and instrumentalities of violations of 52 U.S.C. § 30122 (unlawful straw donations), 52 U.S.C. § 30121 (unlawful foreign contributions), 18 U.S.C. § 371 (conspiracy to commit the same), 18 U.S.C. § 2 (aiding and abetting the same), 18 U.S.C. § 1001 (false statements in a matter within the jurisdiction of the executive branch), 18 U.S.C. § 1343 (wire fraud), 18 U.S.C. § 1346 (honest services fraud), and 18 U.S.C. § 1956 (money laundering) (together, the “Subject Offenses”), including the following:

a. Evidence, including but not limited to communications, relating to contributions made or facilitated by Lev Parnas, Igor Fruman, and/or [REDACTED] on behalf of and/or funded by third parties to political candidates, campaigns, committees or other similar entities.

b. Evidence relating to the sources of the funds used to make contributions in the name of Parnas, Fruman, [REDACTED] or Global Energy Producers LLC (“GEP”).

c. Evidence of Parnas or Fruman’s relationship and/or business dealings with [REDACTED] [REDACTED] Andrey Muraviev, or [REDACTED]

d. Evidence of Parnas, Fruman, or [REDACTED] communications with campaigns, candidates, or PACs.

e. Evidence of Parnas or Fruman attending events sponsored or hosted by, or for the benefit of, [REDACTED] PAC, [REDACTED] PAC, [REDACTED] PAC, [REDACTED] [REDACTED] PAC, and/or [REDACTED] for Congress.

f. Evidence relating to contributions to [REDACTED] PAC, [REDACTED] PAC, [REDACTED] PAC, [REDACTED] PAC, and/or [REDACTED] for Congress.

g. Evidence relating to any request by Parnas or Fruman to [REDACTED] that he take any official action, including but not limited to recommendations relating to the ambassador to Ukraine.

h. Evidence sufficient to establish the ownership of GEP or any related entities, and the extent to which GEP is engaged in the actual operation of an energy business.

i. Evidence sufficient to establish the ownership of bank accounts in the name of [REDACTED] [REDACTED] and/or [REDACTED]

j. Evidence of intent to make unlawful political contributions to violate the campaign finance laws.

k. Evidence of knowledge of the campaign finance laws, including but not limited to knowledge of the prohibition of making contributions in the name of another person, and knowledge of the prohibition on donations or contributions by foreign nationals.

1. Passwords or other information related to online or encrypted messaging.